White Paper KARL STORZ OR1 FUSION® IP

IEC 80001

WHITE PAPER

STORZ
KARL STORZ — ENDOSKOPE

Table of Contents

1 Description - KARL STORZ OR1 FUSION® 3
2 Definition of a ME-system 3
3 Technical Specification - Network Communication and Infrastructure 3
3.1 General 3
3.2 Subnets 4
3.3 DHCP 4
3.4 Bonjour® 4
3.5 Port-based VLAN 5
3.6 Routing between the subnets CONTROL, INTRANET and the Hospital LAN 5
3.7 Multicast Routing between the Intranets 7
3.8 Management Access 7
4 Required Characteristics and Configuration of the Hospital IT Network 8
5 Information flow between KARL STORZ OR1 FUSION® and the Hospital LAN 8
5.1 SIP VOIP-Telephone: 8
5.2 Digital Imaging and Communications in Medicine (DICOM) 9
5.3 Browser 9
5.3.1 KARL STORZ OR1 FUSION® STREAMCONNECT®-Server 9
5.4 PTC Axeda® Connected Access™ Remote Service: 9
5.5 FTP 9
5.6 Network Share (SMB) 9
5.7 Microsoft™ Skype for Business (SfB) 10
5.8 Cisco TelePresence SX80 Codec and SX20 Codec 10
5.9 Network Printer 10
6 Patch Management 10
7 Hazard analysis of the situation 11
7.1 Hazard by malware: 11
7.2 Hazard by incompatible software: 11
7.3 Hazard of data loss: 11
7.4 Hazard of surgical image loss: 11
7.5 Hazard by viewing diagnostic images: 11

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

1 Description - KARL STORZ OR1 FUSION®

KARL STORZ OR1 FUSION® is the name for a product aimed at integrating typical audio-video, documentation and checklist/workflow requirements, features and functionalities for an OR environment into one single integrated system.

2 Definition of a ME-system

A system consists of a combination of networking devices, non-medical devices and ME-systems according ISO/IEC 60601-1 Part 3.64 (Definition of MEDICAL ELECTRICAL (ME) SYSTEM):

[Combination, as specified by its MANUFACTURER, of items of equipment, at least one of which is ME EQUIPMENT to be inter-connected by a FUNCTIONAL CONNECTION or by use of a MULTIPLE SOCKET-OUTLET.]

As defined in Annex H of ISO/IEC 60601-1 the KARL STORZ OR1 FUSION® system is a PEMS (Programmable Electrical Medical System). Therefore the KARL STORZ OR1 FUSION® system, which is isolated from the hospital network via the router, which is provided by KARL STORZ, is completely managed and designed by KARL STORZ. So, the responsibility for the network of the hospital IT administrator ends at the WAN port of the router. A medical system is defined in Clause 16 of ISO/IEC 60601-1.

In Chapter 1, Scope of the ISO/IEC 80001 Note 4, the manufacturer who specifies a ME system that includes a network is responsible for this complete medical system. This is according to the ISO/IEC 60601-1 Part 3.64.

These combinations are tested and verified as a complete system by KARL STORZ.

3 Technical Specification - Network Communication and Infrastructure

3.1 General

The control unit, KARL STORZ OR1 FUSION CONTROL®, has in total three network interfaces, but only one is used for communication with the other devices of the system. The main goal is to create a subnet network structure with galvanic separation if needed. The main goals of the network design are:

1. To separate the IP-traffic (especially the high resolution video transmissions) from the general hospital daily business traffic.
2. Create a subnet network structure with separate networks for Video/Documentation and control devices.
3. Standardized certified configurations for up to 31 OR's.
4. Galvanic separation of the ORs and the central IT components, according to ISO/IEC 60601-1.

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

3.2 Subnets

The intended KARL STORZ OR1 FUSION® network structure consists of four subnets in one OR:

- Hospital LAN (H-LAN). This is the IP infrastructure provided by the customer for the KARL STORZ OR1 FUSION® IP system and becomes a part of the KARL STORZ OR1 FUSION® system. The IP ranges 10.179.0.0/16 must not be used by this subnet.
- BACKBONE network with IP range 10.250.xxx.0/24 will be used by the KARL STORZ OR1 FUSION® system for Inter-OP connection.
- INTRANET with IP range 10.179.xxx.0/24 will be used by the KARL STORZ OR1 FUSION® system for devices intended for Intra-OP connection. (This subnet together with the associated CONTROL subnet is referred to as “System xxx”).
- CONTROL with IP range 192.168.1.0/27. These IPs are identical for every system. The reason for this is that the IPs of the KARL STORZ SCB devices located in every CONTROL subnet can’t be changed by design.
  All devices which are explicitly not involved in Inter-OR connections have to be placed in this subnet. The KARL STORZ SCB *MUST* be on this subnet.

3.3 DHCP

For every system an Extreme Networks[1] Summit Switch offers DHCP-Service for the intranet with IP range 10.179.xxx.11/254.

The DHCP server on the INTRANET provides an automatic IP assignment to the encoder or decoder. Because these devices use the Zeroconf implementation Bonjour® of Apple Inc., the KARL STORZ OR1 FUSION® system identifies them by a symbolic name.

3.4 Bonjour®

The Bonjour®[2] Protocol is Apple’s implementation of the Zeroconf protocol which is used to assign symbolic names associated to an IP like the DNS system but without any centralized server. In combination with DHCP it is used to manage the OR1™ video encoder and decoder from the KARL STORZ OR1 FUSION® software. Because this protocol is based on IP multicasts on the managing IP device (here the Extreme Networks® Switch) it needs IGMP snooping support.

[1] Extreme Networks and BlackDiamond are marks or registered trademarks of Extreme Networks, Inc., in the U.S. and/or other countries
[2] Bonjour® is a registered trademark of Apple Inc.

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

3.5 Port-based VLAN

For higher efficiency the Extreme Networks Summit X670 10G Switch is divided into VLANs. Depending on the customer environment, 1, 2 or 3 ORs may be configured on a single switch. A virtual router will be configured for each OR. Dedicated Control- and Intranet-VLANs are created for an OR. Glass fiber optic connections will be used to set the switch in an own electric domain for galvanic separation, so that no electric fault in one OR can cause an electric failure in another OR.

The following OR configurations are proposed:

- 1 OR per switch. Ports 1-48 are assigned to this OR. Ports 1-5 are reserved for connection with other network devices, so 43 ports remain to connect encoders or decoders to the switch.
- 2 ORs per switch. Ports 1-24 are assigned to the first OR and ports 25-48 to the second OR. Again the first 5 ports of each OR are reserved. The remaining 19 ports per system are available for connecting encoders or decoders to the switch (38 in total).
- 3 ORs per switch. Ports 1-16 are assigned to the first OR, ports17-32 are assigned to the second OR and ports 33-48 are assigned to the third OR. As in the previously described configurations the first 5 ports of each OR are reserved, so 11 ports per system are remaining for connecting encoders or decoders to the switch (33 in total).

All further drawings (Figure 1, Figure 2 and Figure 3) refer to the configuration with three ORs per switch.

3.6 Routing between the subnets CONTROL, INTRANET and the Hospital LAN

As mentioned in chapter 3.5 there is a virtual router for each OR. This virtual router sends the traffic between the control- and intranet-VLAN. Besides these “local” routes the following routes are configured:

- 10.250.xxx.0/24 (local BB-Subnet)
- 10.179.xxx.0/16 (route to the other Intranets)
- 10.179.xxx.2 (default gateway)

Note that there is no route for the devices in the control network to other INTRANET or H-LAN networks. There is no special firewall from an INTRANET to the H-LAN (i.e. all ports can be reached in the H-LAN). Incoming connections to an INTRANET are blocked by the automatic SPI (Stateful Packet Inspection) firewall on the router. Furthermore, the security of the KARL STORZ OR1 FUSION CONTROL® is guaranteed by the NeXus SE46 Software ID software installed on the device. Every IP address can be reached from the KARL STORZ OR1 FUSION® software in the Hospital LAN except the IP addresses used in the CONTROL subnet (IPs 192.168.1.0/).
Because of this, a long subnet prefix (/27) instead of a standard prefix (/24) is used for the CONTROL subnet.

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

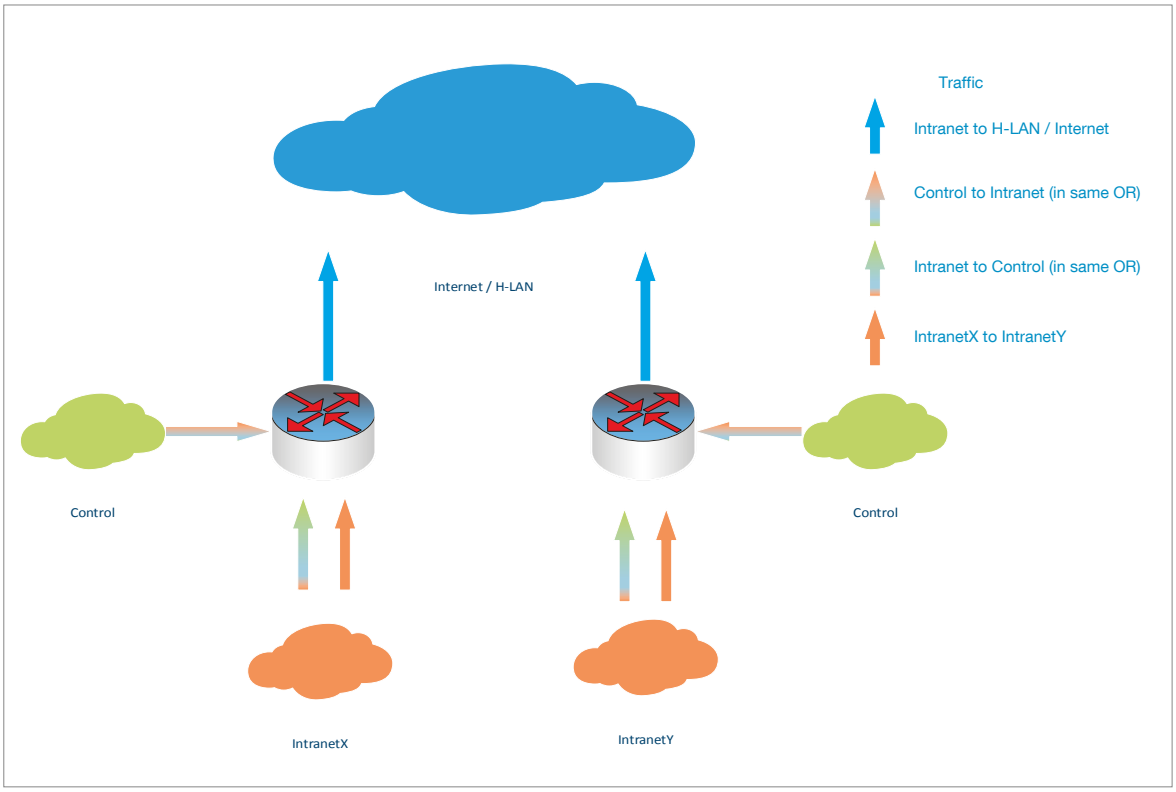

Figure 1: Subnets and the routing in-between

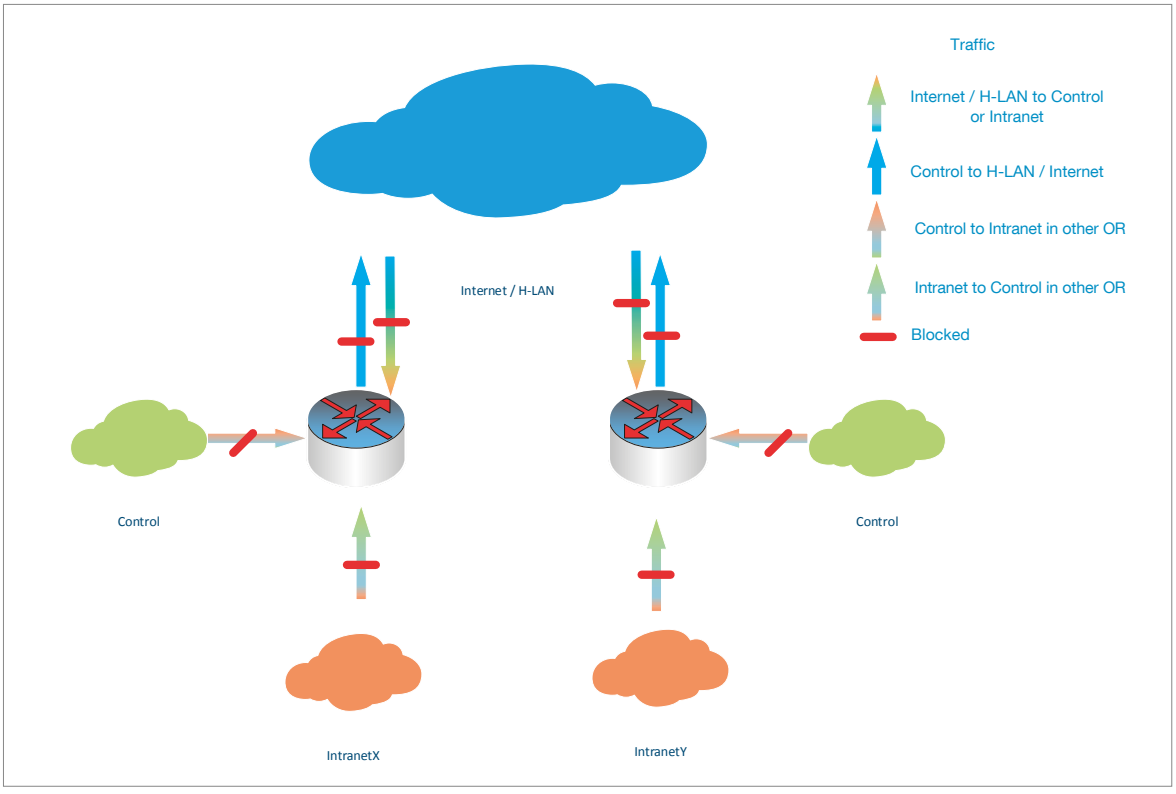

Figure 2: Subnets and routing in-between with firewall

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

3.7 Multicast Routing between the Intranets

To enable room-to-room multicasting, PIM and IGMP are configured for the VLANs on the Extreme Networks Summit Switches. To enhance stability, a loop interface (10.179.0.xxx) for each OR is configured as a static rendezvous point for the broadcast IPs in the OR.

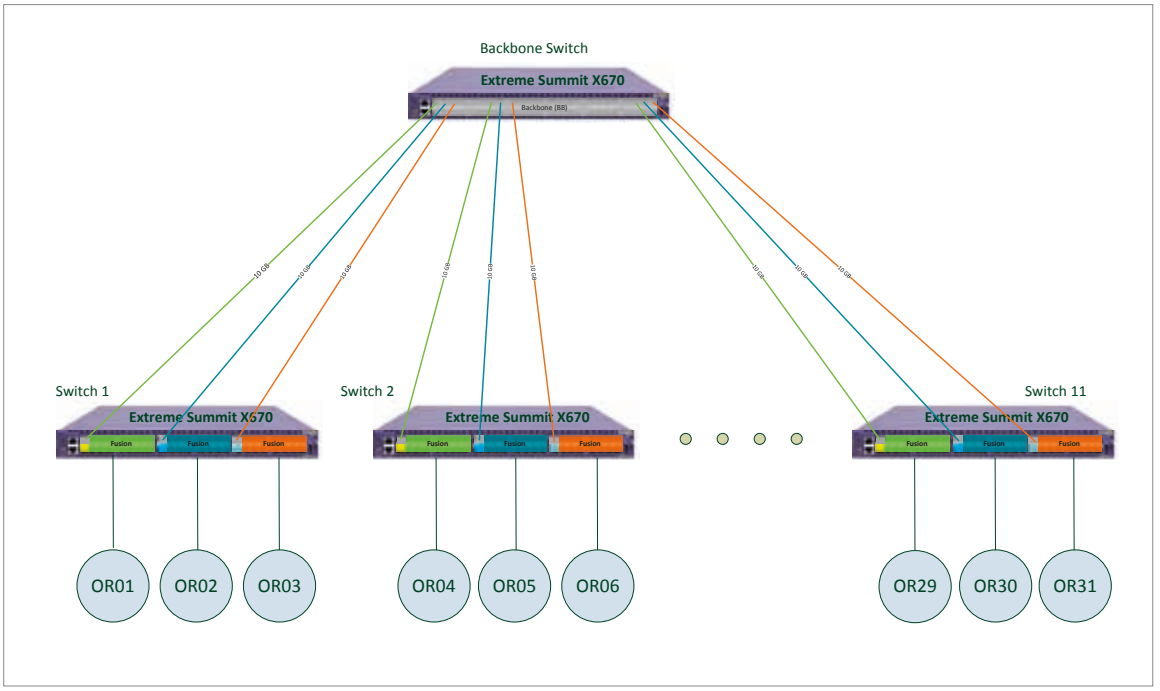

Figure 3: Multicast routing between OP-rooms (physical cabling)

3.8 Management Access

- Through the console port: Settings of the console port: 9600, 8N1, no Hardware or Software Flow Control.
- Through the management port: the management IP of Extreme Networks Summit Switches is 10.0.0.1.
- Create a SSH connection: the Switch accepts only SSH connections from the KARL STORZ OR1 FUSION® PCs, for which there is an OR configured on the switch.
- For Example: Assuming there are 2 ORs (or101 and or122) configured. It is then possible to make a SSH connection from KARL STORZ OR1 FUSION® PC 10.179.101.3 or 10.179.122.3 to 10.179.101.1 or 10.179.122.1, which are the VLAN-IPs configured on the switch.

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

4 Required Characteristics and Configuration of the Hospital IT Network

Refer also to ISO/IEC 80001 (DIN EN 50173; TIA-568)

The following requirements have to be fulfilled by the customer, otherwise correct functionality of the KARL STORZ OR1 FUSION® isn't guaranteed:

- KARL STORZ OR1 FUSION CONTROL® has to be protected with a firewall against unauthorized access from the internet.
- The use of servers with IPs 192.168.1.0/27 for KARL STORZ OR1 FUSION® isn't allowed.
- The use of the subnet 10.179.0.0/16 isn't allowed in the hospital.
- On the POF-to-Copper-Converter only an iPort docking station, a SCB or a Lutron Room Control is allowed.
- QoS for proper VOIP needs to be implemented.
- The availability of a gateway for the KARL STORZ OR1 FUSION® routers has to be guaranteed.
- A maximum round trip time of 300ms has to be guaranteed.
- A minimum bandwidth of 200Mbit/s has to be guaranteed.

5 Information flow between KARL STORZ OR1 FUSION® and the Hospital LAN

The KARL STORZ OR1 FUSION® system supports the following services of external servers in the Hospital LAN or internet:

5.1 SIP VOIP-Telephone:

One of the system features provides the user with an integrated VOIP-Client including local Phone-Book functionality.

The following OR configurations are proposed:

- Required "In-House" SIP server: (e.g. AVAYA Session Manager, Asterisk 1.6, 3CX 11.0 for VOIP telephony.)
- SIP protocol **unencrypted UDP on Port 5060**
- Audio protocol: unencrypted RTP
- Dedicated extension number required

The following Codecs are available at the Client:

PCMA	G722- 16kHz	L 16	G726-24 kHz
PCMU	GSM	G728-8 kHz	G726-32 kHz
Telephone-Event	SPEEX-8kHz	G723-8 kHz	G726-40 kHz
ILBC-8 kHz	SPEEX-16kHz	G726-16 kHz	G729

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

5.2 Digital Imaging and Communications in Medicine (DICOM)

DICOM-server: e.g. DCMTK derived server for saving patient data. For further information see "DICOM Compliance Statement".

5.3 Browser

The browser feature enables access to external web-based content from KARL STORZ OR1™ FUSION®.

However this is only restricted to verified and approved KARL STORZ applications or Third Party Products:

The following applications are enabled:

- KARL STORZ OR1™ STREAMCONNECT® NEO (see Section 5.3.1)

5.3.1 KARL STORZ OR1 FUSION® STREAMCONNECT®-Server

For audio/video communication outside the OR-Environment an additional Server platform is available.

For further information please refer to the country based assigned White Paper:

United States / Canada / Mexico: STREAMCONNECT® NEO

Rest of the world: White Paper OR1™ STREAMCONNECT® II System

5.4 PTC Axeda® Connected Access™ Remote Service:

KARL STORZ offers remote service for the KARL STORZ devices located in the operating room. Connection between devices in the OR and the Axeda®[3] Connected Access™ remote server is established by the device using the https protocol. Further communication between the device and the Axeda® Connected Access™ remote server uses https tunneling.

5.5 FTP

The KARL STORZ OR1 FUSION® system uses passive FTP when exporting data to a FTP server within the IT network infrastructure. That is, all connections are established from the FTP client to the server. Therefore no special firewall configuration of the router is required.

The required FTP credentials to connect to the FTP server need to be configured and stored within the KARL STORZ OR1 FUSION® system.

Please refer to the FTP definition in RFC 959 for more detailed information.

5.6 Network Share (SMB)

The KARL STORZ OR1 FUSION® system uses the SMB protocol standard when exporting data to a network share on a SMB server within the IT network infrastructure. Hereby all connections are established from the SMB client to the server. Therefore no special firewall configuration of the router is required.

The required credentials to connect to the SMB server need to be configured and stored within the KARL STORZ OR1 FUSION® system.

Please refer to the SMB definition by Microsoft under http://msdn.microsoft.com/en-us/library/cc246482.aspx for more detailed information.

[3] Axeda is a registered trademark of Axeda Corporation

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

5.7 Microsoft™ Skype for Business (SfB)

The KARL STORZ OR1 FUSION® system optionally supports a videoconferencing module based on Microsoft™ Skype for Business (SfB). This module consists of a customized client coded to the Lync 2013 API. Therefore, it requires a backend Skype for Business server, whether it be in the cloud (e.g. Microsoft Office 365) or the hospital's own local or remote Skype for Business server. Unique new Skype for Business accounts are created for each OR on the Skype for Business system and the corresponding credentials are entered into the KARL STORZ OR1 FUSION® videoconference modules configuration screen. No other configuration is needed for the router or the KARL STORZ OR1 FUSION® system.

5.8 Cisco TelePresence SX80 Codec and SX20 Codec

The KARL STORZ OR1 FUSION® system provides connections to a Cisco TelePresence SX80 Codec and a Cisco TelePresence SX20 Codec. It controls the Codec over https- and SSH-connections. Audio and video from a conference call via SX80 Codec and SX20 Codec can be routed within the KARL STORZ OR1 FUSION® installation.

5.9 Network Printer

The KARL STORZ OR1 FUSION® system supports the configuration of network printers that can be used for printing treatment reports. The required resources depend on the concrete network printing infrastructure and drivers that are used.

As long as all connections are established from the KARL STORZ OR1 FUSION® system to the network printer no special firewall configuration of the router is required.

The following protocols are tested and verified:

- Network Share (Server Message Block SMB) (see Chapter 6.4)
- Internet Printing Protocol (IPP) **TCP/UDP-Port 631**
- Line Printer Daemon protocol / Line Printer Remote protocol (LPD, LPR) **TCP-Port 515**
- HP-JetDirect **TCP-Port 9100**

6 Patch Management

Classic antivirus protection is only effective if the virus definition file (= blacklist) and the program engine are regularly updated. Therefore, users are only protected against threats that are known to the manufacturer. There is a general risk of a faulty update of the antivirus program negatively affecting the system, resulting in problems as severe as total system failure. Therefore, careful checks are indispensable.

The Patch management solution of the KARL STORZ OR1 FUSION® system is based on **NeXus SE46 Software ID solution,** which starts automatically together with the Windows operating system and uses the whitelist approach. When using a whitelist, all executable files that are not listed on the whitelist are blocked from running. As a result, any intruding malware is prevented from negatively affecting the system or changing it. This includes malware such as viruses or Trojans even if they are hidden in other files.

Only a KARL STORZ service technician has the privileges to switch the **NeXus SE46 Software ID** into the **Service Mode,** which allows full control and sole authorization to make fundamental modifications to the operating system and installations. This also applies to the release of new system components and updates.

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

7 Hazard analysis of the situation

7.1 Hazard by malware:

- Please refer to chapter 6 Patch Management

7.2 Hazard by incompatible software:

- The KARL STORZ OR1 FUSION CONTROL® system is BIOS protected and in KIOSK mode
- The KARL STORZ OR1 FUSION® network is protected and only serviced by KARL STORZ

7.3 Hazard of data loss:

- The KARL STORZ OR1 FUSION® system is not an archiving system
- All information (documents, pictures and streaming media content) have to be exported to USB, CD/DVD, DICOM, network shares

7.4 Hazard of surgical image loss:

- The KARL STORZ OR1 FUSION® network is only serviced by KARL STORZ
- As long as the network connections do not go down, all devices are powered and no device fails, the KARL STORZ network remains stable.

7.5 Hazard by viewing diagnostic images:

- See warnings in user manual - Do not use the KARL STORZ OR1 FUSION® system to view diagnostic images

© KARL STORZ 96202074 OR1 29 1.2 12/2017/EW-E

It is recommended to check the suitability of the product for the intended procedure prior to use.

STORZ
KARL STORZ—ENDOSKOPE
THE DIAMOND STANDARD

KARL STORZ SE & Co. KG
Dr.-Karl-Storz-Straße 34, 78532 Tuttlingen/Germany
Postbox 230, 78503 Tuttlingen/Germany
Phone: +49 (0)7461 708-0
Fax: +49 (0)7461 708-105
E-Mail: info@karlstorz.com

www.karlstorz.com

Health
made in Germany
www.health-made-in-germany.com

96202074 OR1 29 1.2 12/2017/EW-E